REMARKS

Claims 1, 3, 4, 6, 7, 10, 12-14, 18-21, 23-25, 27-29, 31-34, 36, 39, and 41-81 are pending in the present application. The Examiner has objected to claim 19 pursuant to 37 CFR 1.75(c), rejected claims 74-81 pursuant to 35 U.S.C. §112, and rejected claims 42, 43, 56, 68-79 and 81 pursuant to 35 U.S.C. § 102(e) as being anticipated by Kara. In addition, the Examiner has rejected 1, 3, 4, 6, 7, 10, 12-14, 18-21, 23, 27, 32-34, 36, 39, and 41, 44-55, 58-60, and 80, pursuant to 35 U.S.C. § 103(a), as being unpatenable over Kara in view of Talmadge. Finally, the Examiner has rejected claim 63 , pursuant to 35 U.S.C. § 103(a), as being unpatenable over Kara in view of the Information Based Indicia Program System Specification. Applicant respectfully disagrees and requests reconsideration of pending claims 1, 3, 4, 6, 7, 10, 12-14, 18-21, 23-25, 27-29, 31-34, 36, 39, and 41-81 in view of at least the following amendments and remarks.

I. Objection Under 37 C.F.R. 1.75(c)

The Examiner has objected to claim 19 pursuant to 37 C.F.R. 1.75(c). The Examiner states:

> Claim 19 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. See MPEP 608.01(n).
>
> In lines 17-18 of the independent claim 1, it recites that "printing said value-bearing information **while said secure continuous communication link persist.**" (Emphasis added). However, dependent claim 19 recites that "said software sending a print command to said printer **when said communication link disconnects.**" (Emphasis added) which excludes the above limitation recited in the independent claim 1.

Applicant has amended claim 19 in view of the Examiner's comments and now believes the objection is moot.

II. Rejection of Claims 74-81 based on 35 U.S.C. §112(2)

The Examiner has rejected claims 74-81 under 35 U.S.C. §112 second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. The Examiner states:

> Claims 74, it is not clear what the difference is between "client system software" in line 2 and "client system software" in line 6.

Applicant has amended claim 74 in view of the Examiner's comments and now believes the rejection is moot.

III. Rejection of Claims 42, 43, 56, 68, 69-79 and 51 Based on 35 U.S.C. §102(e)

The Examiner has rejected independent claims 42, 43, 56, 68, 69-79 and 81 under 35 USC 102(e) as being anticipated by Kara (U.S. Patent 5,822,739) stating:

> Re: claim 42: Kara discloses a secure on-line postage management method comprising:
> establishing a secure continuous communication link between a client system and a server system *(col. 6, lines 11-22)*;

said client system processing a user request for obtaining an indicium *(col. 6, lines 11-22);*

said client system securely communicating said user request to said server system *(col. 6, lines 11-22);*

said server system processing said user request *(col. 6, lines 37-43);*

said server system securely communicating to said client system a response to said user request *(col. 6, lines 11-22);*

said client system processing said response to obtain said indicium *(col. 6, lines 11-22), "decrypting the received data packet");*

said client system obtaining said indicium while said secure continuous communication link persists *(col. 11, lines 6-12 and lines 18-21 and receiving data packet);* and

said client system printing said indicium while said secure continuous communication link persists *(col. 11, lines 6-12 and lines 18-21 and printing the desired postage indicia).*

Re claim 69: Kara discloses a method having steps of establishing a secure continuous communication link between a client system and a server system *(col. 6, lines 11-17),* wherein said client system comprises client system software *("Demand" program);* said client system software presenting one or more options for submitting at least one payment *(col. 13, lines 31-45);* submitting said at least one payment to said server system software while said secure continuous communication link persists *(col. 13, lines 25-30 and 31-45);* adding postage value corresponding to an amount of said at least one payment to a user account *(col. 13, lines 25-30 and 31-45, i.e., credit account for later billing);* and printing at least one indicia representative of said postage while said secure continuous communication link persists *(col. 11, lines 6-12 and lines 18-21 and printing the desired postage indicia).*

Re claim 74: Kara discloses a computer program product having a computer readable medium having client system software *i.e., "a data communications program")* embodied therein, said client system software configured to: establish a secure continuous communication link between a client system and a server system *(col. 6, lines 11-17)* comprising server system software *(i.e., "a meter program"),* wherein said client system comprises client system software *(i.e., "Demand program")* configured to present one or more options for submitting at least one payment *(col. 13, lines 31-45);* said client system configured to submit at least one payment to said server system software while said continuous communication link persists between said client system and said server system *(col. 6, lines 11-17; col. 13, lines 25-30 and 31-45, i.e., "a data communication program" processes information);* said server system software configured to credit postage value corresponding to an amount of said at least one payment to a user account *(col. 6, lines 11-17; col. 13, lines 25-30 and 31-45, i.e., "a data communication program" processes information);* and said client system software printing at least one indicia representative of said postage value while said secure continuous communication link to said server system software persists *(col. 11, lines 6-12 and lines 18-21 and printing the desired postage indicia).*

Applicant respectfully disagrees and submits that independent claims 42, 69, and 74, as amended, are not anticipated by the Kara reference because Kara

does not teach suggest or describe the steps of monitoring a secure continuous communication link between a first computer and a second computer and terminating the client software when the secure communication link is not continuous.

IV. Rejection of Claims 1, 3, 4, 6, 7, 10, 12-14, 18-21, 23, 27, 32-34, 36, 39, 41, 44-55, 58-60, and 80 Based on 35 U.S.C. §103(a)

The Examiner has rejected claims 1, 3, 4, 6, 7, 10, 12-14, 18-21, 23, 27, 32-34, 36, 39, 41, 44-55, 58-60, and 80 based on 35 U.S.C. §103(a) as being unpatentable over Kara (U.S. Patent 5,822,739), in view of Talmadge (U.S. Patent 4,858,138), stating:

> Kara discloses a secure on-line printing method, comprising:
> establishing a communication link between a first computer and a second computer *(i.e., claim 27, the step of "coupling said first system to a second processor-based system");*
> executing a client software on said first computer, wherein said client software initiates a secure continuous communication link between said first computer and said second computer *(col. 6, lines 11-17; col. 11, lines 6-12 and 18-21);*
> sending a request for value bearing information from said client software to said second computer *(i.e., claim 27, the step of "transmitting said demand from said first system to said second system");* and
> sending value-bearing-information from said second computer to said first computer in response to said request *(i.e., claim 27, the step of "transmitting said data packet from said second system to said first system"),* while said communication link is continuous *(col. 11, lines 13-18);* and printing said value-bearing information while said secure continuous communication link persists *(col. 11, lines 6-12 and lines 18-21 and printing the desired postage indicia).*
>
> Further, Kara discloses a secure on-line postage metering method comprising:
> establishing a secure communication link between a user computer and a vendor computer *(i.e., claim 27, the step of "coupling said first system to a second processor-based system" and using an encryption module);*
> providing a printer connected to said user computer *(printer 24);*
> executing an on-line postage metering software on said user computer wherein said on-line postage metering software determines if said secure

communication link between said first computer and said computer is continuous *(col. 6, lines 11-17; col. 11, lines 6-12 and 8-21);*

said on-line postage metering software *(i.e., "Demand program")* sending a request for a print authorization to said vendor computer *(i.e., claim 27, the step of "transmitting said demand from said first system to said second system");*

said vendor computer accessing a database to verify fund availability to cover said request *(col. 13, lines 31-45);*

said vendor computer sending data elements for a postage indicium to said first computer as a response to said request *(i.e., claim 27, the step of "transmitting said data packet from said second system to said first system");* and

said on-line postage metering software sending a postage indicium graphic associated with said data elements to said printer while said secure continuous communication link persists *(i.e., "Demand program" decrypting the received data packet for printing and col. 11, lines 6-12 and 18-21).*

Re claim 1: Kara does not explicitly disclose the steps of monitoring said secure continuous communication link between said first and said second computer and terminating said client software when said communication link is not continuous. However, Talmadge discloses the steps of monitoring said secure continuous communication link between said first and said second computer and terminating said client software when said communication link is not continuous to secure vault having electronic indicia *(e.g., the system having means for disabling the host module from activating the print means to print said indicia unless said vault module is coupled thereto as claim 20 would inherently monitor whether the link between the vault module and the host module is continuous or not).* Thus, it would have been within the level of ordinary skill in the art to modify the method of Kara by adopting the teaching of Talmadge to further enhance the security of the claimed method.

Re claims 32, 36 and 41: Kara does not explicitly disclose the step of terminating said online postage metering software when said communication link is not continuous, said on-line postage metering software disabling a print spooler of said printer, and said online postage metering software sending a print cancel command to said printer if said secure communication link is interrupted. However, Talmadge discloses the step of disabling the printer connected to said first computer to secure vault having electronic indicia *(e.g., claim 20).* Thus, it would have been within the level of ordinary skill in the art to modify the method of Kara by adopting the teaching of Talmadge to further enhance the security of the claimed method.

Applicant respectfully disagrees and submits that independent claims 1 and 32 are allowable for at least the following reasons.

1. Kara and Talmadge, either alone or in any combination, do not teach, suggest, or describe client system software or postage metering software

that monitors a secure continuous communication link between a first computer and a second computer and terminates the client software when the secure communication link is not continuous.

Applicant agrees with the Examiner's statement that "Kara does not explicitly disclose the steps of monitoring a secure continuous communication link between a first computer and a second computer and terminating the client software when the secure communication link is not continuous" and respectfully submits that the Talmadge reference also lacks these same steps.

The Examiner states that Talmadge teaches a "system having the means for disabling the host module from activating the print means to print said indicia unless said vault module is coupled thereto as claim 20 would inherently monitor whether the link between the vault module and the host module is continuous or not". Applicant respectfully disagrees with the Examiner's conclusion and submits that the second part of the statement made by the Examiner, "as claim 20 would inherently monitor whether the link between the vault module and the host module is continuous or not", is not a correct interpretation of Talmadge.

The invention described in Talmadge is a postage printing meter, referred to as a "value printing system", consisting of two modules, one representing a postage meter or "electronic vault" and the other a mailing machine that actually

prints the postage. Both modules are physically housed together as a part of the value printing system. Talmadge states that means are provided to disable the host module from activating a printing means to print postage unless the vault module is coupled to the host module. Talmadge does not state that the vault module monitors a secure continuous communication link between a first computer and a second computer and terminates the client software when the secure communication link is not continuous. As shown in Figure 4 of Talmadge, the meter transmits a serial number, validation number and fixed indicia pattern to the host and then ceases to operate. Once this data has been received by the host, as shown in Figure 3, the postage is printed in a separate step. No monitoring by the meter is indicated in Figure 3 and there is no way of preventing the printing of postage once the data has been transmitted from the meter to the host. The meter has no way of terminating printing once the host has been activated.

Talmadge provides a means to disable the host from activating the printing means (see e.g., claim 20). Once the printing means has been activated, Talmadge does not possess a way to subsequently monitor printing or terminate printing. This is also stated at column 6, lines 24 – 29, where Talmadge states:

not in claim 1

> Thereafter the printer 17 (FIG. 1) will print on the document 3 the fixed portion of the postage indicia 19, the dollar amount 22, the date 23, the meter serial number 21, and the validation number 24 received from the meter 1, box 46.

The text states the printer will print, with no provision for monitoring or terminating printing. For these reasons, Applicant respectfully submits that Talmadge does not teach, suggest, or describe client system software or postage metering software that monitors a secure continuous communication link between a first computer and a second computer and terminates the client software when the secure communication link is not continuous.

The Examiner has admitted that Kara does not explicitly disclose the steps of monitoring a secure continuous communication link between a first computer and a second computer and terminating the client software when the secure communication link is not continuous. Talmadge's meter activates the host and thereafter the host is free to print postage on its own without further monitoring or supervision and without being subject to having the printing terminated by the meter. Therefore, Applicant respectfully submits that Kara and Tallmadge, either alone or in any combination, fail to teach, disclose or suggest the claimed invention.

The MPEP states at Section §2143, page 2100 - 97:

> To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.

Applicant respectfully submits that a prima facie case of obviousness has not been established. The Examiner has proposed to combine the prior art in the Kara and Talmadge because "it would have been within the level of ordinary skill in the art to modify the method of Kara by adopting the teaching of Talmadge to further enhance the security of the claimed method". However, adopting the teachings of Talmadge would not create the claimed invention because Talamadge's meter activates the host and thereafter the host is free to print postage on its own without requiring further monitoring or supervision and without aborting the printing if the secure communication link is dropped. Accordingly, there is no way to combine the Kara and Talmadge references to accomplish the claimed invention. For example, consider how the combination of Kara and Talmadge would function. Following Kara and Talmadge, a combined system would provide for a postage metering system, containing a meter and a host, where the host would be activated and would thereafter be free to print postage without supervision by the meter and without being subject to being terminated by the meter. Clearly, the combination of Kara and Talmadge cannot teach the claimed invention because it is missing the key steps of monitoring the printing of postage and retaining the ability to terminate the host when the communication link is no longer continuous. The preceding paragraphs demonstrate that the prior art references relied upon by the Examiner, even when combined, do not teach or suggest all the claim limitations as required by MPEP §2143, quoted above. Therefore, Applicant respectfully request that claims 1, 3, 4, 6, 7, 10, 12-14,

18-21, 23, 27, 32-34, 36, 39, 41, 44-55, 58-60, and 80 be placed in condition for allowance.

V. Rejection of Claim 63 in view of Kara and the Information Based Indicia Program System Specification (IBIPSS hereinafter: October 9, 1996, The United States Postal Service)

The Examiner has rejected claim 63 under 35 U.S.C. §103(a) as being rendered obvious by Kara (US Pat. 5,822,739) in view of the Information Based Indicia Program System Specification (IBIPSS hereinafter: October 9, 1996, The United States Postal Service) stating:

> Re claim 63: Kara discloses an on-line postage system for processing of user requests and obtaining postage indicia comprising:
> a client system *(a first processor-based system)* for interfacing with a user;
> a server system *(a second processor-based system)* in continuous and secure communication with said client system, comprising *(col. 6, lines 11-22)*:
> a communication server for communicating with client system *(col. 7, lines 18-36;*
> a database server for storing user information *(col. 14, lines 24-30);*
> a transaction server for processing of requests communicated to said server system by said client system *(col. 14, lines);*
> a cryptographic device for encrypting communication between said client system and said server system *(col. 6, lines 20-23, i.e., "decrypting the received data packet" implies that the second processor-based system must have a cryptographic device);*
> a continuous communication link with a financial management system for processing user payments *(col. 13, lines 45-50, i.e., "the provider will demand payment from the bank card company concurrent with the postage demand.").*
>
> Kara does not explicitly disclose either a firewall for ensuring the integrity of said server system against potential unauthorized access or a continuous communication link with the United States Postal Service Central Meter Licensing System (USPS CMLS) for licensing of a user. However, as shown by IBIPSS *(see page 3-13, section 3.2.6.3)*, the open system server shall prompt the user to apply for a postage meter license and update the license as required by the DMM. Thus, it would have been obvious to one of ordinary skill in the art to establish a continuous communication link with the United States Postal Service Central Meter Licensing System (USPS CMLS) for licensing of a user to satisfy the requirement. Further, the communication link must be continuous with the

> USPS CMLS until the licensing of the user is finalized. Still further, Kara states that the server system can be used by a plurality of remotely located client systems and the client system provides security system to prevent unauthorized utilization of the postage metering system *(col.4, lines 36-51)*. Of course, a firewall is one of the well-known security systems in the art and the use of this well known feature at the server system would have been within the level of ordinary skill in the art, since it has been held that rearranging parts of an invention involves only routine skill in the art. *In re Japikse*, 86 USPQ 70.

Applicant has amended claim 63 to emphasize the differences between the invention and the prior art and respectfully disagrees that Kara and IBIPSS, either alone or in combination teach, suggest, or describe an online postage system as claimed. None of the references cited describe an online postage system that contains a private network subsystem having a communication server configured to communicate information to at least one financial management institution. Moreover, the references cited do not describe a cryptographic hardware device, but rather describe cryptographic modules each of these distinctions are further elaborated upon below:

1. Kara, either alone or in combination with the IBIPSS reference, does not teach, suggest or describe an online postage system that has a communication server within a private network subsystem for communicating with at least one financial management system.

The invention as claimed is directed to an online postage system having a communication server within a private network subsystem for communicating with at least one financial management system. Both Kara and the IBIPSS

reference cited by the Examiner lack any description of a private network subsystem that is part of an online postage system. For example, the references cited do not restrict access to certain segments of the online postage system while leaving other parts of the system publicly accessible. Such separation between different aspects of the online postage system is accomplished in one or more embodiments of the invention through the use of a firewall configured to ensure the integrity of the system by restricting access between the public network subsystem and a private network subsystem.

The Examiner admits that "Kara does not explicitly disclose either a firewall for ensuring the integrity of the server system against potential unauthorized access or a continuous communication link with the United States Postal Service Central Licensing Meter System (USPS CMLS) for licensing of users", but concludes that "a firewall is one of the well-known security systems in the art and the use of this well known feature at the server system would have been within the level of ordinary skill in the art, since it has been held that rearranging parts of an invention involves only routine skill in the art. *In re Japikse,* 86 USPQ 70." Applicant respectfully disagrees that the use of a firewall in the manner that is claimed was well known in the art at the time of invention and requests that the Examiner provide references supporting this conclusion. In the claimed invention, the firewall functions within the server system as an internal boundary between the private subsystem and the public subsystem. Thus, the firewall segments the system into a private network subsystem and a

public network subsystem where the private network subsystem contains a communication server, a transaction server and a database so that requests to sensitive information in the database can be accessed from the transaction server without allowing for access by those who have authority to access to public network subsystem. Applicant respectfully submits that such use does not conform to that which was known in the art at the time of filing.

Another difference between the claimed invention and both Kara and the IBIPSS reference is that the claimed invention calls for a communication server within the private network subsystem for communicating with at least one financial management institution whereas the references cited provide for no such communication server in the manner that is claimed. For instance, the references lack a communication server capable of communicating with a financial institution's financial management system through some type of continuous communication link. The Examiner states that Kara's PC 20 can be equated to a communication server (See e.g., Column 7, lines 18-36). However, Applicant respectfully disagrees. Kara's PC 20 cannot be equated with the communication server of the claimed invention because PC 20 is not a communication server within a private network subsystem for communicating information to at least one financial management system. Kara does not have servers that are part of a private network subsystem and configured with such functionality. The IBIPSS reference also makes no mention of servers configured with such functionality. Therefore, Kara, either alone or in combination with

IBIPSS, cannot teach, suggest or describe an online postage system that comprises a communication server within a private network subsystem enabled with one or more protocols to allow for communicating information between the postage system and a financial management system. Accordingly, Applicant respectfully requests that the present case be placed in condition for allowance.

2. Kara, either alone or in combination with IBIPSS, does not teach, suggest or describe the use of cryptographic hardware device.

The Examiner cites column 6, lines 20-23 of Kara as the basis for rejecting the claim language "a cryptographic device for encrypting communication between said client system and said server system." The Examiner states "'decrypting the received data packet' implies that the second processor-based system must have a cryptographic device." Applicant respectfully disagrees that the cited portion of Kara describes a cryptographic device as claimed. A cryptographic device is different than the cryptographic module described in Kara. The term cryptographic module as used in Kara refers to a software program configured to utilize cryptographic key sets for purposes of encrypting or decrypting data. In contrast, the invention claims a cryptographic hardware device configured to provide a greater degree of protection for security relevant data items. The crpytographic device also includes physical tamper resistance and active anti-tampering mechanisms. This distinction is significant because

using a hardware based cryptographic device provides additional security above and beyond the use of the software-based encryption systems described in Kara.

An example of the benefits conferred by using a cryptographic hardware device are discussed at pages 100 , lines 16-25 and page 101, lines 1-4. The specification states "The cryptographic process employed in one embodiment of the current_invention is based on public key cryptography and a cryptographic hardware device 23340 or 23440 (StampMaster PSD), which meets the FIPS 140-1 level 3 requirements for operation and level 4 requirements for physical security. The cryptographic devices 23340 and 23440 incorporated in the server 180 infrastructure provide high performance Data Encryption Standard (DES) and Rivest Shamir Adleman (RSA) cryptographic processing. The cryptographic processes are performed within a secure enclosure that is designed to meet the stringent requirements of FIPS 140-1 security level 4. All software operating with the cryptographic device's secure environment is first authenticated using digital signature techniques." This passage illustrates that a cryptographic device provides a significant level of additional security above and beyond the cryptographic module referred to in Kara. In contrast to the cryptographic device as claimed, Kara cannot, for instance, provide a secure enclosure that limits physical access to the device and thereby any data processed by the device. Accordingly, for at least the reasons stated above, Applicant respectfully submits that Kara does not teach, suggest, or describe the invention as claimed. The IBIPSS reference mentions that indicia may contain a digital signature algorithm

flag. However, IBIPSS also does not disclose a cryptographic device for encrypting communication between said client system and said server system.

B. Dependent Claims 3, 4, 6, 7, 10, 12-14, 18-21, 23-25, 27-29, 31, 33, 34, 36, 39, 41, 43-62, 64-68, 70-73, and 75-81

Applicant respectfully submits that claims 3, 4, 6, 7, 10, 12-14, 18-21, 23-25, 27-29, 31, 33, 34, 36, 39, 41, 43-62, 64-68, 70-73, and 75-81 being dependent upon respective allowable base claims are allowable for at least the aforementioned reasons.

CONCLUSION

For at least the above aforementioned reasons, Applicant respectfully submits that pending claims 1, 3, 4, 6, 7, 10, 12-14, 18-21, 23-25, 27-29, 31-34, 36, 39, and 41-81 are patentably distinct from the prior art of record and in condition for allowance. Applicant therefore respectfully requests that pending claims 1, 3, 4, 6, 7, 10, 12-14, 18-21, 23-25, 27-29, 31-34, 36, 39, and 41-81 be placed in condition for allowance.

Very truly yours,

THE HECKER LAW GROUP

Date: August 28, 2002

Cynthia A. Casby
Reg. No. 47,475

THE HECKER LAW GROUP
1925 Century Park East
Suite 2300
Los Angeles, California 90067
(310) 286-0377

CERTIFICATE OF MAILING

This is to certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as First Class Mail in an envelope addressed to Assistant Commissioner for Patents, Washington, D.C. 20231 on August 28, 2002.

Signature: Deanna Blizzard
Date: August 28, 2002 8-28-02

MARKED-UP VERSION OF CLAIMS IN ACCORDANCE WITH 37 CFR 1.121(c)(1)(ii)

+121E

CLAIMS

1. (UNCHANGED) A secure on-line printing method, comprising:

establishing a communication link between a first computer and a second computer;

executing a client software on said first computer, wherein said client software initiates a secure continuous communication link between said first computer and said second computer;

monitoring said secure continuous communication link between said first computer and said second computer;

terminating said client system software when said secure communication link is not continuous;

sending a request for value bearing information from said client software to said second computer;

sending said value-bearing information from said second computer to said first computer in response to said request, while said secure communication link is continuous; and,

printing said value-bearing information while said secure continuous communication link persists.

2. (CANCELED)

MARKED-UP VERSION OF CLAIMS IN ACCORDANCE WITH 37 CFR 1.121(c)(1)(ii)

3. (UNCHANGED) The method of claim 1 wherein said request comprises encrypted data.

4. (UNCHANGED) The method of claim 3 wherein said value-bearing item information comprises encrypted data.

5. (CANCELED)

6. (UNCHANGED) The method of claim 3 wherein said value-bearing information comprises an image of a postal indicium.

7. (UNCHANGED) The method of claim 6 wherein said request comprises a postage amount

8. (CANCELED)

9. (CANCELED)

10. (UNCHANGED) The method of claim 1 wherein said sending said request for said value bearing information is in response to command from a user.

MARKED-UP VERSION OF CLAIMS IN ACCORDANCE WITH 37 CFR 1.121(c)(1)(ii)

11. (CANCELED)

12. (UNCHANGED) The method of claim 7 wherein said second computer comprises a database containing user information.

13. (UNCHANGED) The method of claim 12 wherein said user information comprises financial information associated with said user.

14. (UNCHANGED) The method of claim 13 wherein said sending said request to said second computer further comprises accessing said user information to verify fund availability to cover said postage amount.

15. (CANCELED)

16. (CANCELED)

17. (CANCELED)

18. (UNCHANGED) The method of claim 14 wherein said value-bearing information comprises disabling a print spooler of a printer connected to said first computer.

MARKED-UP VERSION OF CLAIMS IN ACCORDANCE WITH 37 CFR 1.121(c)(1)(ii)

19. (ONCE AMENDED) The method of claim 18 further comprising said client software sending a print command to said printer when said secure continuous communication link disconnects.

20. (UNCHANGED) The method of claim 1 wherein said value-bearing information comprise ticket information

21. (UNCHANGED) The method of claim 20 wherein said request comprises a ticket price.

22. (CANCELED)

23. (UNCHANGED) The method of claim 1 wherein said second computer sends authorization to said first computer in response to said request, said second computer accessing said user's financial information to verify funds availability.

24. (UNCHANGED) The method of claim 1 wherein said value-bearing information comprise check information.

25. (UNCHANGED) The method of claim 24 wherein said request comprises a check amount.

MARKED-UP VERSION OF CLAIMS IN ACCORDANCE WITH 37 CFR 1.121(c)(1)(ii)

26. (CANCELED)

27. (UNCHANGED) The method of claim 1 further comprising:

accessing said user's financial information to verify funds availability to cover said value-bearing information;

sending said authorization to said first computer.

28. (UNCHANGED) The method of claim 1 wherein said value-bearing information comprises coupon information.

29. (UNCHANGED) The method of claim 28 wherein said request comprises a coupon amount.

30. (CANCELED)

31. (UNCHANGED) The method of claim 1 wherein said information comprises certificate information.

32. (UNCHANGED) A secure on-line postage metering method comprising:

establishing a secure communication link between a user computer and a vendor computer;

providing a printer connected to said user computer;

MARKED-UP VERSION OF CLAIMS IN ACCORDANCE WITH 37 CFR 1.121(c)(1)(ii)

executing an on-line postage metering software on said user computer wherein said on-line postage metering software determines if said secure communication link between said first computer and said second computer is continuous;

terminating said on-line postage metering software when said communication link is not continuous;

said on-line metering software sending a request for a print authorization to said vendor computer;

said vendor computer accessing a database to verify fund availability to cover said request;

said vendor computer sending data elements for a postage indicium to said first computer as a response to said request;

said on-line postage metering software sending a postage indicium graphic associated with said data elements to said printer while said secure continuous communication link persists.

33. (UNCHANGED) The method of claim 32 wherein said on-line postage metering software sending said request comprises encrypting said request.

34. (UNCHANGED) The method of claim 32 wherein said vendor computer sending said response further comprises encrypting said response.

MARKED-UP VERSION OF CLAIMS IN ACCORDANCE WITH 37 CFR 1.121(c)(1)(ii)

35. (CANCELED)

36. (UNCHANGED) The method of claim 32 further comprising: said on-line metering software disabling a print spooler of said printer.

37. (CANCELED)

38. (CANCELED)

39. (UNCHANGED) The method of claim 32 wherein said on-line postage metering software sending said request for said print authorization is in response to a command from a user.

40. (CANCELED)

41. (UNCHANGED) The method of claim 32 further comprising said on-line postage metering software sending a print cancel command to said printer if said secure communication link is interrupted.

42. (THREE TIMES AMENDED) A secure on-line postage management system method comprising:

establishing a secure continuous communication link between a client system and server system;

monitoring said secure continuous communication link between said client system and said server system;

terminating client system software when said secure communication link is not continuous;

said client system processing a user request for obtaining an indicium;

said client system securely communicating said user request to said server system;

said server system processing said user request;

said server system securely communicating to said client system a response to said user request;

said client system processing said response to obtain said indicium;

said client system obtaining said indicium while said secure continuous communication link persists;

said client system printing said indicium while said secure continuous communication link persists.

43. (UNCHANGED) The method of claim 42 wherein said client system securely communicating with said server system comprises:

MARKED-UP VERSION OF CLAIMS IN ACCORDANCE WITH 37 CFR 1.121(c)(1)(ii)

authenticating a user by a establishing said secure communication link between said client system and said server system and verifying the authenticity of information exchanged;

continuously monitoring said secure communication link to verify said authenticity of information exchanged.

44. (ONCE AMENDED) The method of claim 43 wherein said authenticating said user comprises:

said client system obtaining a password;

securely sending said password to said server system;

said client system issuing a challenge to said server system;

said server system modifying said challenge cryptographically;

said client system verifying said modified challenge for proper authentication of the communication.

45. (UNCHANGED) The method of claim 44 wherein said sending said password comprises sending said password to said server using triple Data Encryption Standard (DES) of the SSL Internet protocol, thereby establishing an SSL triple DES communication session between said client system and said server system.

MARKED-UP VERSION OF CLAIMS IN ACCORDANCE WITH 37 CFR 1.121(c)(1)(ii)

46. (UNCHANGED) The method of claim 45 wherein said client system issuing a challenge comprises issuing a 64 bit random number to said server system.

47. (UNCHANGED) The method of claim 46 wherein said server modifying said challenge comprises said server system digitally signing said challenge using a cryptographic module and a private key associated with said server system.

48. (UNCHANGED) The method of claim 47 wherein said client system verifying said modified challenge comprises using a public key corresponding to said private key associated with said server system to verify said digital signature of said challenge.

49. (UNCHANGED) The method of claim 43 wherein said continuously monitoring said secure communication link comprises:

said server system retrieving a password associated with said client system;

generating a message authentication code using said password associated with said client system;

sending said message authentication code and said challenge to said client system;

said client system verifying said authentication code using said challenge and said password associated with said client system.

50. (UNCHANGED The method of claim 49 wherein said retrieving said password further comprises:

retrieving said password from a database;

decrypting said password if said password is encrypted.

51. (UNCHANGED) The method of claim 50 wherein said message authentication code is generated using said password associated with said client system.

52. (TWICE AMENDED) The method of claim 42 wherein said secure continuous communication link between said client system and said server system is established through a firewall.

53. (UNCHANGED) The method of claim 42 wherein said secure continuous communication between said client system and said server system is established via the Internet secure sockets layer (SSL) protocol.

MARKED-UP VERSION OF CLAIMS IN ACCORDANCE WITH 37 CFR 1.121(c)(1)(ii)

54. (UNCHANGED) The method of claim 42 wherein said server system processing said user request takes place in a public network and a private network included within said server system.

55. (UNCHANGED) The method of claim 54 wherein said public network processes said user requests independently from said private network to protect the integrity of said server system.

56. (UNCHANGED) The method of claim 42 wherein said secure communication between said client system and said server system is encrypted.

57. (UNCHANGED) The method of claim 42 wherein said secure communication between client system and server system is encrypted by a United States Postal Service compliant cryptographic device.

58. (UNCHANGED) The method of claim 42 further comprising disabling said client system from obtaining said indicium if said secure continuous communication between client system and server system is discontinued.

59. (UNCHANGED) The method of claim 54 wherein said private network processes said user requests for making payments.

MARKED-UP VERSION OF CLAIMS IN ACCORDANCE WITH 37 CFR 1.121(c)(1)(ii)

60. (UNCHANGED) The method of claim 59 wherein said private network processes said users requests for making payments further comprises communicating with a financial management system for verification of availability of funds and fund transfer.

61. (UNCHANGED) The method of claim 42 further comprising said server system communicating with the United States Postal Central Meter Licensing System (USPS CMLS) for processing of user licensing information.

62. (UNCHANGED) The method of claim 61 further comprising registering a said user.

63. (THREE TIMES AMENDED) An on-line postage system for processing of user requests and obtaining postage indicia comprising:

a client system for interfacing with a user;

a server system in continuous and secure communication with said client system, said server system having an architecture comprising:

a communication server within a private network subsystem for communicating ~~with the client~~ information to at least one financial management system;

a database server for storing user information within said private network subsystem;

MARKED-UP VERSION OF CLAIMS IN ACCORDANCE WITH 37 CFR 1.121(c)(1)(ii)

a transaction server within a public network subsystem for processing of requests communicated to said server system by said client system;

a firewall for ensuring the integrity of said server system ~~against potential unauthorized access~~ by restricting access between said public network subsystem and said private network subsystem;

a cryptographic hardware device for encrypting communication between said client system and said server system;

a continuous communication link with the United States Postal Service Central Meter Licensing System (USPS CMLS) for licensing a user;

a continuous communication link with ~~a~~ said at least one financial management system for processing user payments.

64. (UNCHANGED) The on-line postage system of claim 63 further comprising a system software down-loadable from said server system to said client system.

65. (UNCHANGED) The on-line postage system of claim 63 wherein said client system interfaces with at least one user.

66. (UNCHANGED) The on-line postage system of claim 63 wherein said server system is accessible through an Internet portal.

MARKED-UP VERSION OF CLAIMS IN ACCORDANCE WITH 37 CFR 1.121(c)(1)(ii)

67. (UNCHANGED) The on-line postage system of claim 63 wherein said client system comprises administration software to monitor said client system.

68. (UNCHANGED) The method of claim 42 wherein said client system obtaining said indicium comprises:

maintaining a said continuous communication link between said client system and said server system; and

retrieving said indicium from said server system.

69. (TWICE AMENDED) A method comprising:

establishing a secure continuous communication link between a client system and a server system, wherein said client system comprises client system software;

monitoring said secure continuous communication link between said client system and said server system;

terminating said client system software when said secure communication link is not continuous;

said client system software, presenting one or more options for submitting at least one payment;

submitting said at least one payment to said server system software while said secure continuous communication link persists;

adding postage value corresponding to an amount of said at least one payment to user account;

printing at least one indicia representative of said postage value while said secure continuous communication link persists.

70. (UNCHANGED) The method of claim 69 further comprising:

deducting said amount from said user account.

71. (UNCHANGED) The method of claim 70 wherein said deducting is performed upon authorization from said user.

72. (UNCHANGED) The method of claim 69 wherein said at least one payment comprises credit card data.

73. (UNCHANGED) The method of claim 69 wherein said at least one payment comprises electronic funds transfer data.

74. (TWICE AMENDED) A computer program product comprising:

a computer readable medium having [client system] software embodied therein, said [client system] software configured to:

establish a secure continuous communication link between a client system and a server system comprising server system software, wherein said client

system comprises client system software configured to present one or more options for submitting at least one payment;

monitor said secure continuous communication link between said client system and said server system;

terminate said client system software when said secure communication link is not continuous;

said client system configured to submit said at least one payment to said server system software while said secure continuous communication link persists between said client system and said server system;

said server system software configured to credit postage value corresponding to an amount of said at least one payment to a user account;

said client system software printing at least one indicia representative of said postage value while said secure continuous communication link to said server system software persists.

75. (UNCHANGED) The computer program product of claim 74 further comprising said client system software configured to deduct said amount from said user account.

76. (UNCHANGED) The computer program product of claim 74 wherein said submitting is performed by said client system software upon authorization from said user.

MARKED-UP VERSION OF CLAIMS IN ACCORDANCE WITH 37 CFR 1.121(c)(1)(ii)

77. (UNCHANGED) The computer program product of claim 74 wherein said payment comprises credit card data.

78. (UNCHANGED) The computer program product of claim 74 wherein said payment comprises electronic funds transfer data.

79. (UNCHANGED) The computer program product of claim 74 wherein said secure continuous communication link utilizes Internet protocols to transfer data.

80. (UNCHANGED) The computer program product of claim 74 wherein said client system software prohibits transmission if said secure continuous communication link fails authentication.

81. (UNCHANGED) The computer program product of claim 74 wherein data transmitted between said client software and said server system software comprises encrypted information.